FISMA and Metrics

Samuel A. Merrell , CISSP, GSEC

25 October 2007

Federal Information Assurance Conference

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
25 OCT 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
FISMA and Metrics	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University ,Software Engineering Institute (SEI),Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
present at the 2007 Federal Information Assurance Conference (FIAC), October 2007 in College Park, MD.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**96**	

Software Engineering Institute

Established in 1984

Federally Funded Research and Development Center (FFRDC)

FFRDC sponsored by the Office of the Secretary of Defense (OUSD AT&L) and operated by Carnegie Mellon University on a five-year renewable contract -- one of 10 FFRDCs sponsored by the Department of Defense

Chartered to work with both government and private sector to transfer important new technology so that the government can benefit from a wider, broader base of expertise

SEI Operations

Works with the private sector under a *Collaborative Agreement* between respective firm and Carnegie Mellon University.

All agreements require the approval of the SEI DoD sponsor

Non-degree-granting, college-level unit of Carnegie Mellon University (~550 employees)

Carnegie Mellon University owns all intellectual property created by the SEI; USG receives a free-to-use license

~$100M enterprise

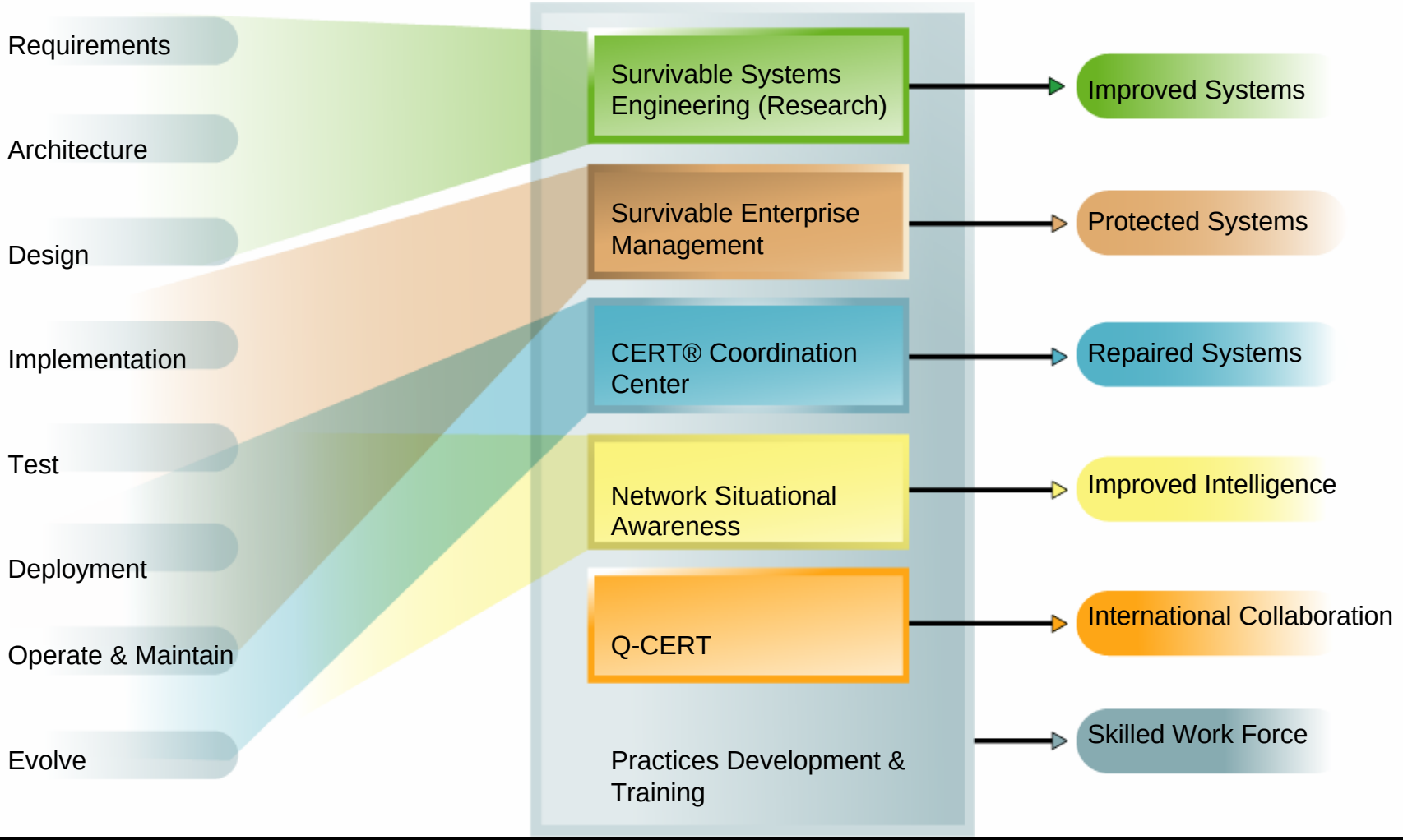
Operations

Established in 1988 and currently the largest of five technical programs within the SEI (~140 employees)

Some key audiences:

- National defense and intelligence community
- Federal civilian agencies
- Federal law enforcement
- Critical infrastructure protection
- Financial services industry
- Incident response teams with national responsibility

Program


Requirements
Architecture
Design
Implementation
Test
Deployment
Operate & Maintain
Evolve
Survivable Systems Engineering (Research)
Survivable Enterprise Management
CERT® Coordination Center
Network Situational Awareness
Q-CERT
Practices Development & Training
Improved Systems
Protected Systems
Repaired Systems
Improved Intelligence
International Collaboration
Skilled Work Force

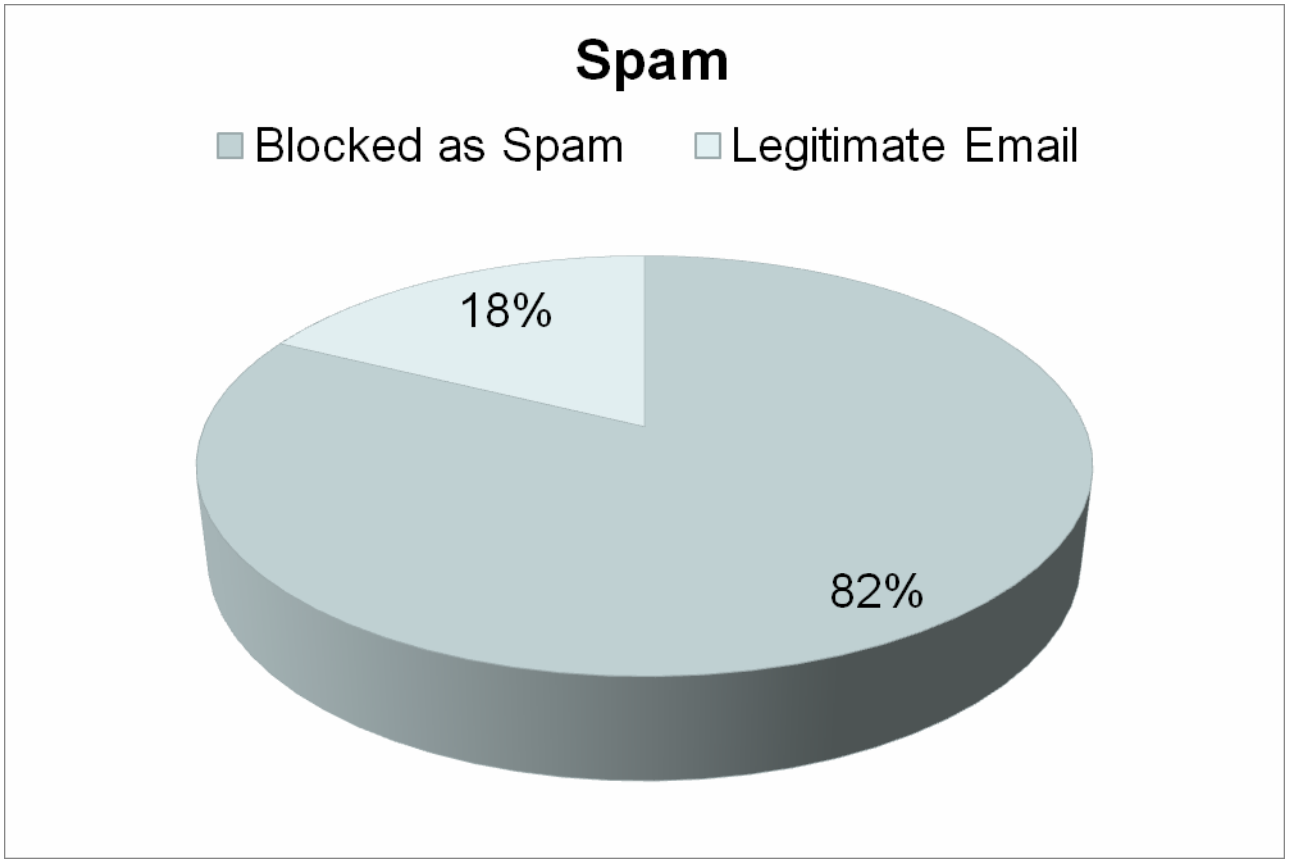
Survivable Enterprise Management

- Assist organizations in developing and implementing approaches to enterprise security management improvement
- Establish techniques and approaches for risk-based requirements elicitation and analysis
- Promote and transition OCTAVE self-directed security evaluation method
- Research the risks posed to information systems/organizations by insiders
- Improve security management capabilities through the development of an enterprise security management capabilities framework (Resiliency Engineering Framework or REF)

- http://www.cert.org/work/organizational_security.html

Introduction to Metrics and Measurements

Introduction to Metrics and Measurements



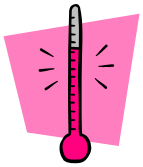
Agenda

- Overview
- NIST Guidance
  - SP 800-55
  - SP 800-80
  - SP800-55, Revision 1
- Intro to Process Maturity and CMMI
- Measurement and Analysis Process Area of CMMI
- Conclusion

Terms

Measurement- Information that is generated by counting things.

"*It is 95 degrees*"



Metric- Information that is derived through analysis that is applied to measurements

"*Today was the hottest day of the year*"

"Metrics 101" presentation by Elizabeth A. Nichols, CTO ClearPoint metrics, May 2006

Why Are We Discussing Metrics and Measurements?

Information Security Metrics, when done well:

- Enables better decision making
- Indicates program performance, both good and bad
- Justifies resource allocation
- Gauges control implementation
- Provides evidence of risk management
- Eases reporting efforts
  - FISMA
- "Demonstrates management commitment" *–NIST SP 800-55*

What is a “Good Metric?”

- A Good Metric is a consistent standard for measurement. It should have the following characteristics:
  - Consistently measured
  - Cheap to gather
  - Expressed as a number or percentage
  - Expressed using at least one unit of measure”[1]
  - Relevant[2]

1 “**Security Metrics: Replacing Fear, Uncertainty, and Doubt**” Andrew Jaquith © 2007 Pearson Education, inc.

2 “ Metrics 101” presentation by Elizabeth A. Nichols, CTO ClearPoint metrics, May 2006

Your organization **is not ready for a metrics program** if:

You do not have :

- A clear, formal understanding of your goals
  - Strategic Plans
  - Policies
  - Procedures
  - Guidelines
- Existing, repeatable processes
- Open lines of communication with stakeholders

Overview of the Federal Information Security Management Act (FISMA)

Federal Information Security Management Act

TITLE III—INFORMATION SECURITY

SEC. 301. INFORMATION SECURITY.

‘‘SUBCHAPTER III—INFORMATION SECURITY

‘‘§ 3541. Purposes

‘‘The purposes of this subchapter are to—

‘‘(1) provide a comprehensive framework for ***ensuring the effectiveness of information security controls*** over information resources that support Federal operations and assets;”

NIST Guidance

Special Publication 800-55 “Security Metrics Guide for Information Technology Systems”

SP 800-55 “Security Metrics Guide for Information Technology Systems” - History

- Released in July 2003
- Originated from GISRA compliance workshops in 2002

SP 800-55 “Security Metrics Guide for Information Technology Systems” – Purpose 1

- Intended to guide the development, selection, and implementation of *system level* metrics.
- IT Security Metrics are designed to:
  - Facilitate decision making
  - Improve performance and accountability
- Mapped metrics to NIST SP 800-26 critical elements

SP 800-55 “Security Metrics Guide for Information Technology Systems” – Purpose 2

- SP800-55 is designed to help an organization:
  - Identify the adequacy of existing controls, policies, and procedures
  - Decide where to invest resources
  - Identify and evaluate nonproductive controls
  - Develop and implement metrics
  - Adequately justify security investments
  - Satisfy FISMA requirements to state performance measures for past and current fiscal years

“Implementation of an IT Security Metrics program will demonstrate agency commitment to proactive security.”

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Security Metrics Program Structure[1]

Security Metrics Program Structure

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Security Metrics Program Structure$_2$

Upper level management support is critical

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Security Metrics Program Structure$_3$

Practical policies need to be backed by authority

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Security Metrics Program Structure[4]

Metrics must be based on goals and objectives

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Security Metrics Program Structure[5]

Emphasize consistent periodic review of data

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Program Requirements

*"The success of an **information security program** implementation should be judged by the degree to which meaningful results are produced."*

Success Factors:

1. **Organizational Consideration**
   - Stakeholders part of program development and implementation
2. **Manageability**
   - Organizations should prioritize measurement requirements
   - Ensure that a limited number of metrics are gathered (10-15)
3. **Data Management Concerns**
   - Standardized methods for metrics data collection and reporting

SP 800-55 "Security Metrics Guide for Information Technology Systems" – IT Security Metrics Requirements

Metrics must:

- Be based on IT Security goals and objectives
- Yield quantifiable information

Data must:

- Be readily obtainable

The processes must:

- Be measurable

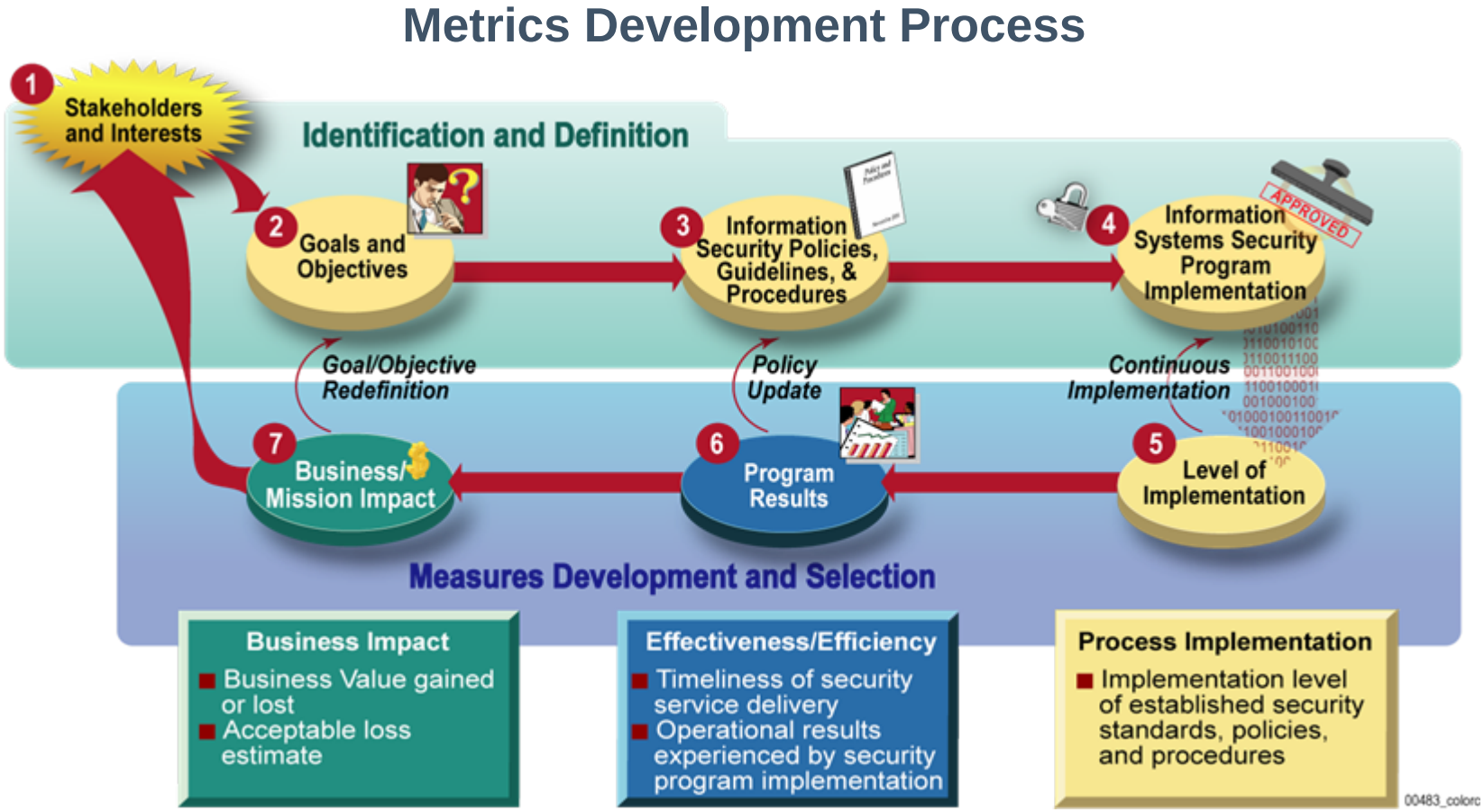
SP 800-55 “Security Metrics Guide for Information Technology Systems” – Metrics Development Process$_1$

Metrics Development establishes the initial set of metrics

Two Major Activities:

1. Identification and development of current IT Security Program
2. Development and selection of specific metrics that measure:
   - **Implementation** of controls
   - **Efficiency** and **effectiveness** of controls
   - **Impact** of controls

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Development Process$_2$



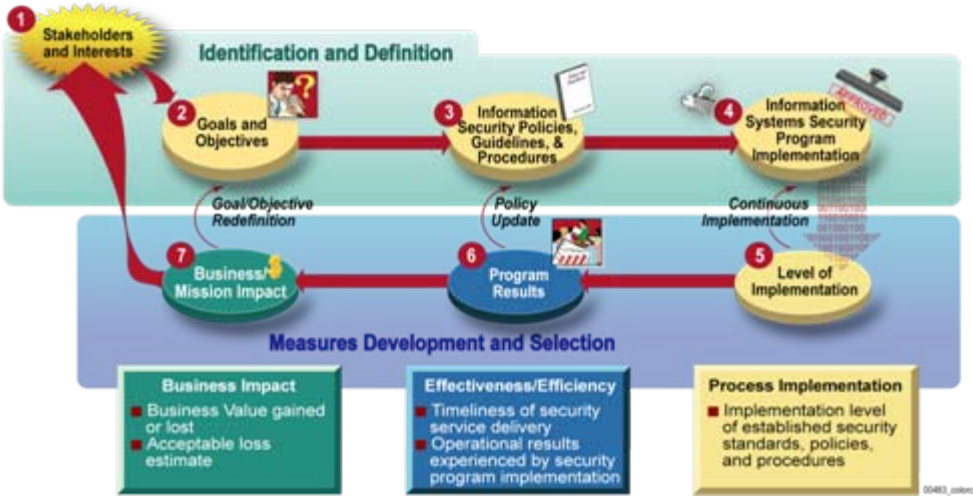
Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Development Process$_3$

Stakeholder identification

Anyone within an organization

- Primary stakeholders
  - Agency Head
  - CIO
  - ISSO
  - System Owners
- Secondary stakeholders
  - CFO
  - Training
  - HR



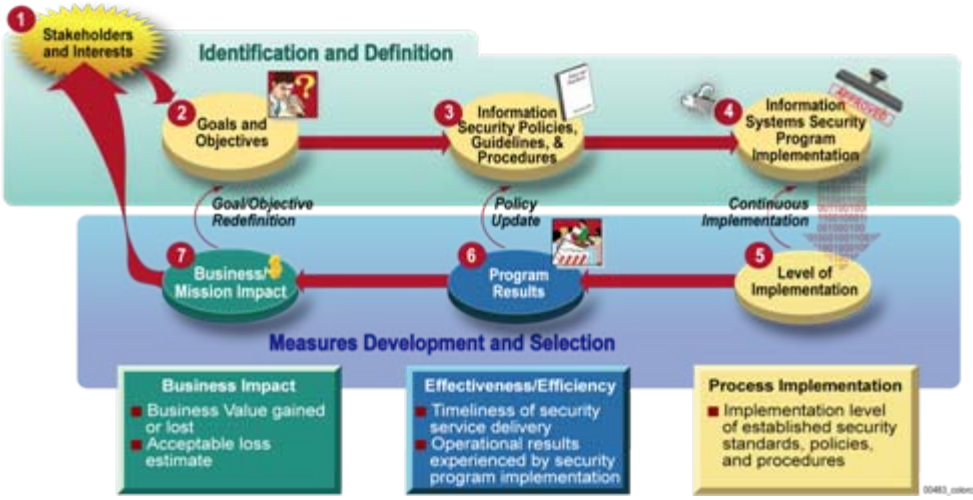
Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Development Process$_4$

Goals and Objectives Definition

Expressed as high level policies and requirements, including:

- **Clinger-Cohen Act**
- **Presidential Decision Directives**
- **FISMA**
- **NIST Special Publications**



Graphic from NIST SP 800-55

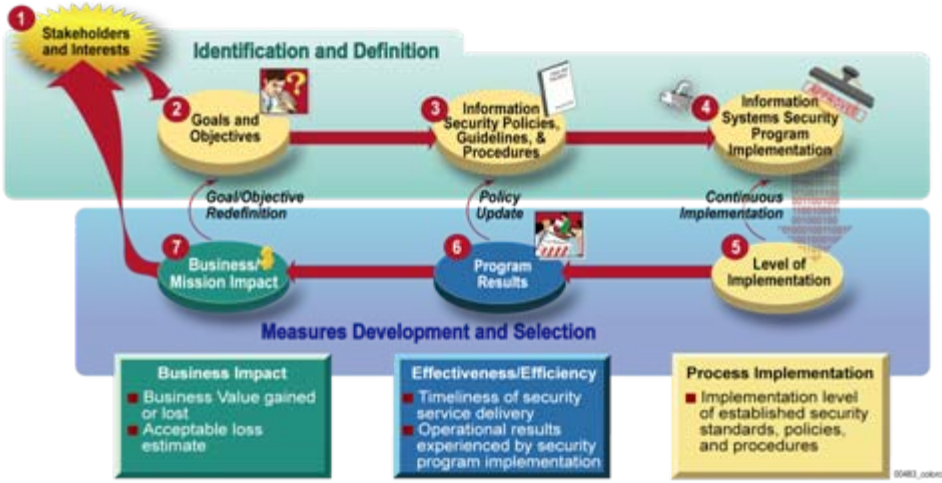
SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Development$_5$

IT Security Policies, Guidance, and Procedures

Organization specific documents define a baseline of security practices.

Identify:

- Prescribed practices
- Applicable targets of performance
- Detailed security controls for system operations and maintenance



Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Development Process$_6$

System Security Program Implementation Review

Includes:

System Security Plans

POA&M documents

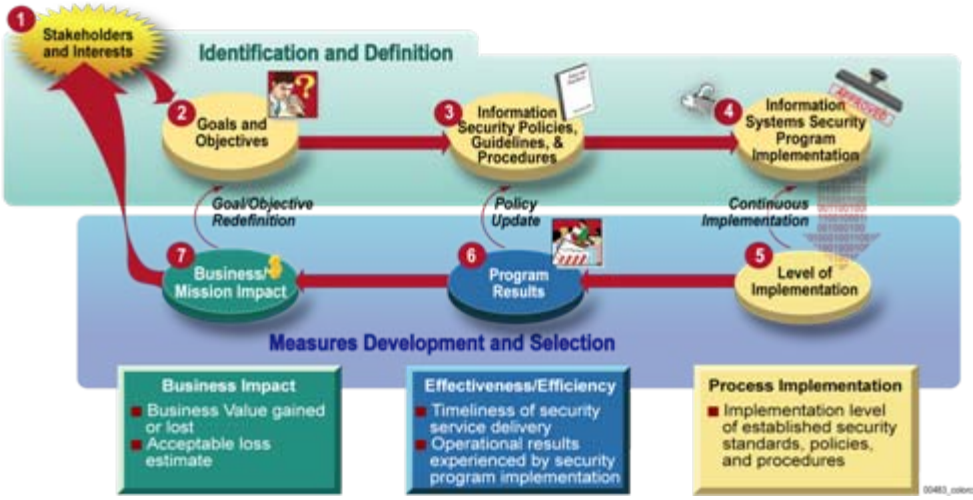
Latest IG findings

Risk assessments

COOP plans

C&A documents

Training results



Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Development Process[7]

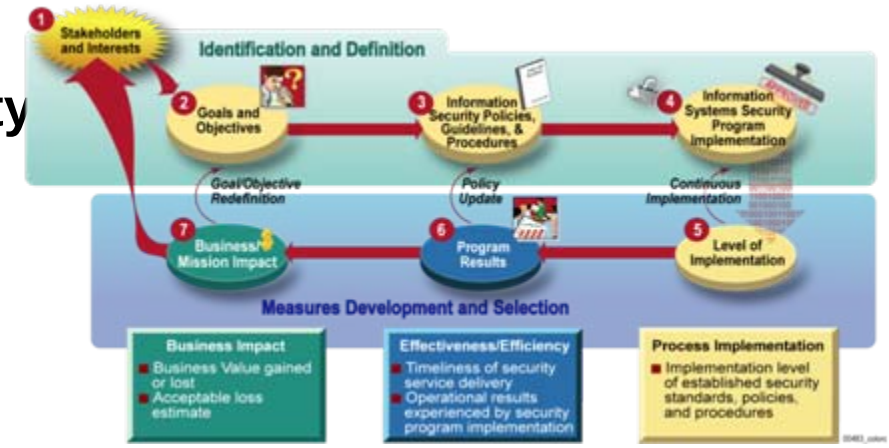
Metrics Development and Selection

Metrics measure

- Process implementation
- Effectiveness
- Efficiency
- Mission Impact

Prioritize metrics based on:

- Their ability to facilitate security control implementation
- The ease of obtaining them
- Existing, stable processes



Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Development Process$_8$

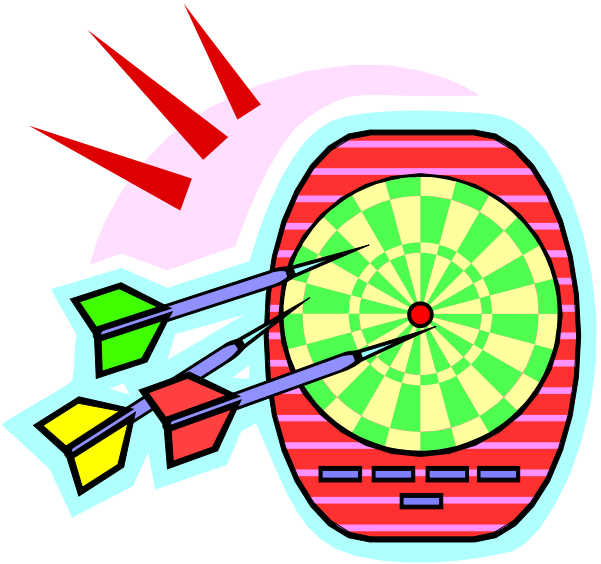
Establishing Performance Targets

Implementation Metrics

- Set at 100% completion of specific tasks

Efficiency, Effectiveness, and Impact Performance Metrics

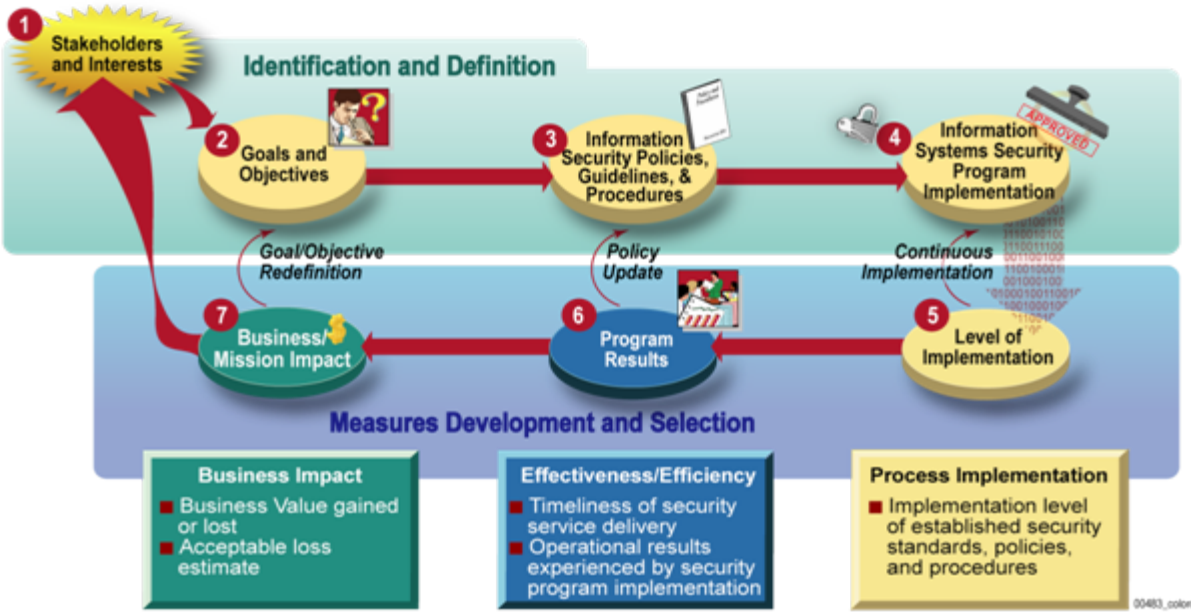
- Management needs to determine goals for performance
- Targets need to be reviewed and adjusted



SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Development Process[10]

An agency's initial set of metrics must:

- Facilitate improvement of control implementation
- Use data that can realistically be obtained
- Measure stable, existing processes

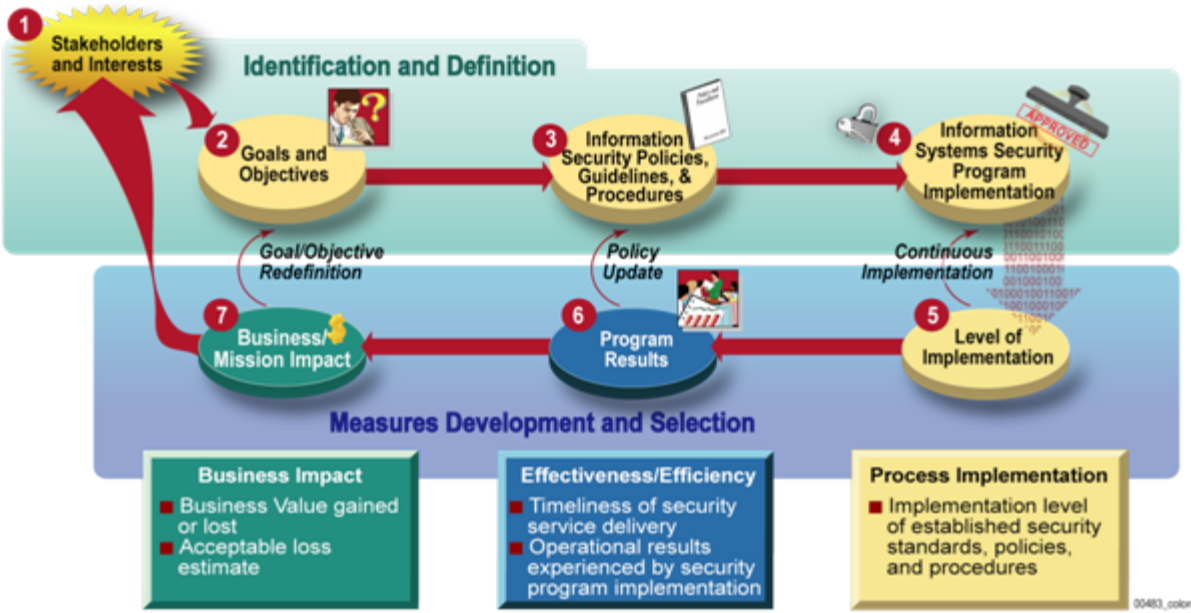


Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Development Process$_{11}$

Feedback Within the Metrics Development Process

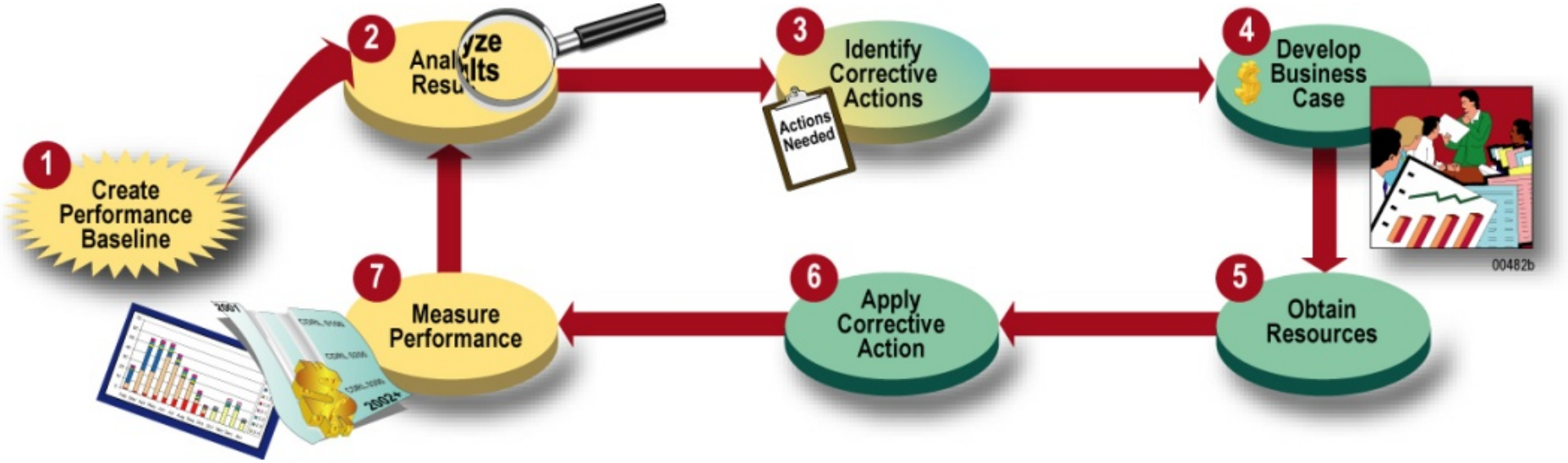
- Metrics will facilitate an understanding of whether the security performance goals are appropriate



Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Program Implementation[1]

Metrics Program Implementation



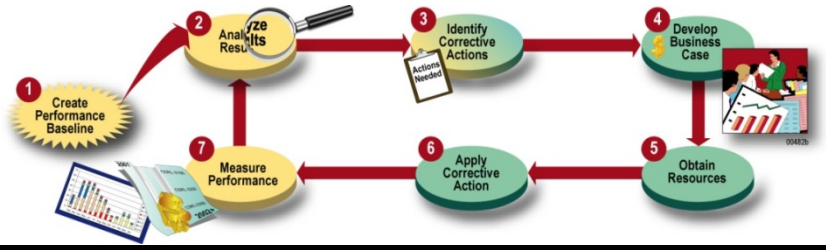
Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Program Implementation$_2$

Create Performance Baseline

Metrics Program Implementation Plan

- Intended audience
- Data collection, analysis, and reporting plan
- Inter- and intra- office coordination
- Creation and/or selection of tools
- Modification of any tools
- Metrics summary reporting formats



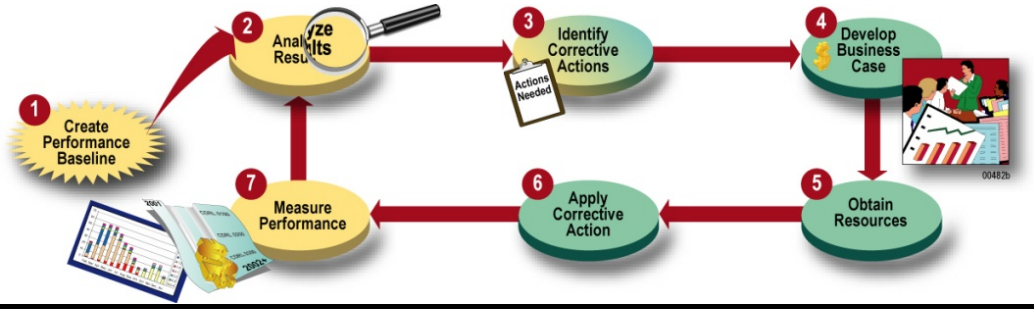
Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Program Implementation$_3$

Analyze Results

Ensure that collected metrics are used to understand system security and identify improvement actions

- Collect data
- Consolidate data and store it
- Conduct a gap analysis
- Identify causes of poor performance
- Identify opportunities for improvement



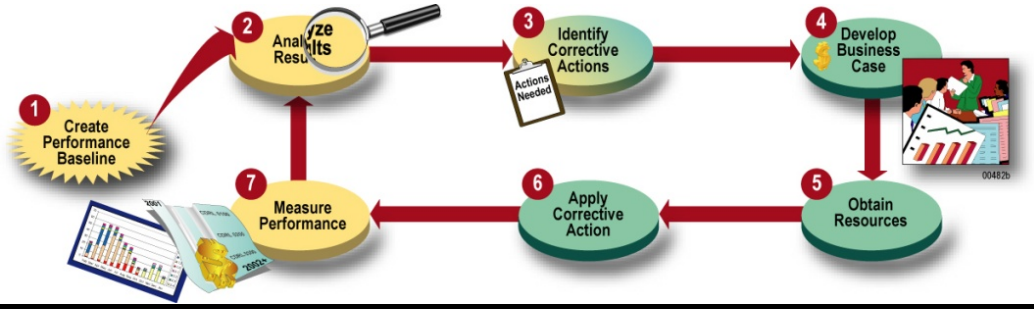
Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Program Implementation$_4$

Identify Corrective Actions

Develop a roadmap how to close implementation gaps

- Determine the range of possible corrective actions for gaps
- Prioritize corrective actions based on risk (800-30)
- Select most appropriate corrective action

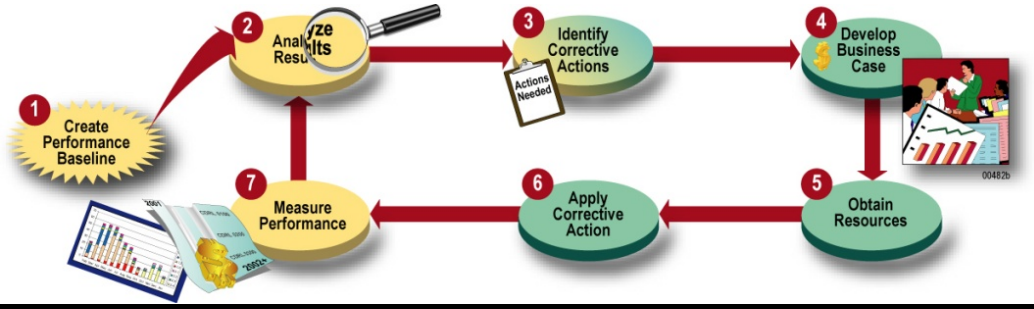


Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Program Implementation$_5$

Develop Business Case and Obtain Resources

- Document mission objectives
- Determine the cost of the status quo as a baseline
- Document gaps between target performance and current state
- Estimate costs for each proposed alternative
- Characterize benefits
- Risk assessment on alternatives
- Prepare budget submission
- Assign resources



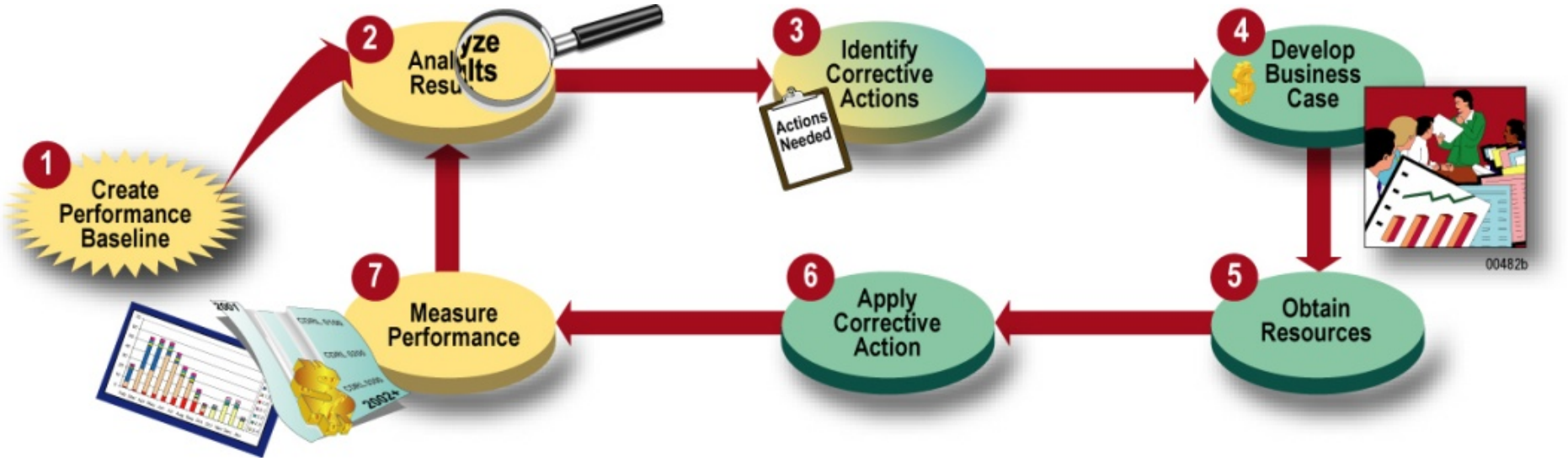
Graphic from NIST SP 800-55

SP 800-55 "Security Metrics Guide for Information Technology Systems" – Metrics Program Implementation, 7

Apply Corrective Actions

"Second verse, same as the first!"

– Herman's Hermits



Graphic from NIST SP 800-55

Special Publication 800-80
"Guide for Developing Performance Metrics for Information Security"

SP 800-80 ”Guide for Developing Performance Metrics for Information Security” - History

- Released as a public draft in May of 2006
- Intended to be a companion to SP 800-55
- Will not be released as a final version (superseded by 800-55R1)

SP 800-80 ”Guide for Developing Performance Metrics for Information Security” - Purpose

- Focuses on developing and implementing information security metrics for an information security program, linking information security performance to agency performance by leveraging agency strategic planning
- Performance metrics provide the means for tying information security activities to strategic goals
- Outlined an agency information security metrics program
- Based on the controls that were introduced in 800-53

SP 800-80 ”Guide for Developing Performance Metrics for Information Security” 800-80 vs. 800-55

800-55 guidance applies primarily to the development of metrics for individual systems

- Defines three types of metrics for individual systems
  - Implementation Metrics
  - Effectiveness and Efficiency Metrics
  - Impact Metrics

800-80 guidance applies to an information security program

- Describes two ways of developing metrics at the program level

SP 800-80 ”Guide for Developing Performance Metrics for Information Security” – Performance Metrics Approach$_1$

Control-Specific Approach

- Mapped to an individual 800-53 control
- Implementation metric

Cross-Cutting Approach

- Based on more than one individual control or family
- Provide a broader view of the information security program
- Can map to goals and objectives related to performance

SP 800-80 ”Guide for Developing Performance Metrics for Information Security” Control-Specific Candidates

- Percentage of system users that have received basic awareness training (AT-4)
- Percentage of information security personnel who have received security training (AT-4)
- Average frequency of audit records review for analysis for inappropriate activity (AU-6)
- Percentage of audit log findings reported to appropriate officials (AU-6)
- Percentage of systems that are compliant with the baseline configuration (CM-2)
- Percentage of new systems that completed C&A prior to implementation (CA)

SP 800-80 ”Guide for Developing Performance Metrics for Information Security” Cross-Cutting Candidates

- Percentage of SP 800-53 Control Families for which policies exist
- Percentage of employees who have signed an acknowledgement that they have read the policies

Break

SP 800-55, Revision 1
"Performance Measurement Guide for Information Security"

SP 800-55, Revision 1 “Performance Measurement Guide for Information Security” - History

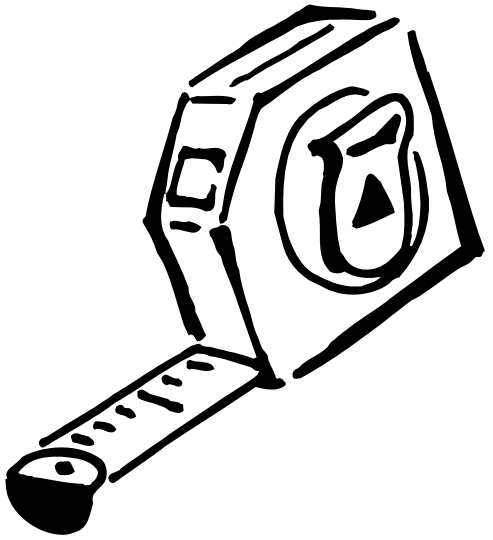
- Draft released in September, 2007
- Supersedes both 800-55 and 800-80

SP 800-55, Revision 1 “Performance Measurement Guide for Information Security” Purpose

- Purpose is to assist in the development, selection, and implementation of measures to be used at the information system and program levels
- Still focuses on SP 800-53’s Control Families, but states that the guidance can be used to develop agency-specific measures related to security controls not included in 800-53
- Inherits elements of both 800-55 and 800-80
- Reflects NIST’s increased focus on enterprise information security programs.

SP 800-55, Revision 1 “Performance Measurement Guide for Information Security” New Vocabulary

Measures - the results of data collection, analysis and reporting



SP 800-55, Revision 1 “Performance Measurement Guide for Information Security” - Measures Background

Information security measures monitor the accomplishment of goals and objectives by:

- Quantifying implementation, efficiency, and effectiveness of security controls
- Analyzing the adequacy of program activities
- Identify possible improvement actions

Measures must:

- Yield quantifiable information (percentages, numbers)
- Involve easily obtainable data
- Provide relevant performance trends over time

SP 800-55, Revision 1 “Performance Metrics Guide for Information Security” - Benefits of Measures

- Increased accountability
- Improved information security effectiveness
- Demonstrate compliance and commitment
- Provide Inputs for resource allocation

SP 800-55, Revision 1 "Performance Metrics Guide for Information Security" - Types of Measures$_1$

Implementation measures- used to demonstrate progress in implementing information security programs, specific security controls, and associated policies and procedures

- *Percentage of systems with approved System Security Plans*
- *Percentage of systems with a standard configuration*

SP 800-55, Revision 1 "Performance Metrics Guide for Information Security" - Types of Measures$_2$

Efficiency/Effectiveness Measures **-**monitor results of security control implementation.

- *Percentage of enterprise operating system vulnerabilities for which patches have been applied or that have been otherwise mitigated*
- *Percentage of incidents caused by improperly configured access controls*

These measures address not only the result of control implementation, but the timeliness of the control

SP 800-55, Revision 1 "Performance Metrics Guide for Information Security" - Types of Measures$_3$

Impact Measures- *combine information about the implementation of controls with information about resources*

- *Cost Savings*
- *Public Trust*
- *Mission-related impacts*

Percentage of the agency's information system budget devoted to information security

Percentage of E-Gov security and Privacy milestones met

Percentage of remote access points used to gain unauthorized access

Percentage of FISP 199 moderate and high impact systems that have successfully tested contingency plans within the past year

A Very Brief Introduction to Process Maturity and CMMI

A brief introduction to process maturity and the $CMMI_1$

- Premise- The quality of a system is highly influenced by the quality of the process used to acquire, develop, and maintain it.
- Process improvement increases product and service quality as organizations apply it to achieve their business objectives.
- Process improvement objectives are aligned with business objectives.

CMMI Benefits

The CMMI Product Suite is at the forefront of process improvement because it provides the latest best practices for product and service development and maintenance. CMMI best practices enable organizations to do the following:

A Brief Introduction to Process Maturity and the $CMMI_3$

- More explicitly link management and engineering activities to their business objectives
- Expand the scope of and visibility into the product lifecycle and engineering activities to ensure that the product or service meets customer expectations
- Incorporate lessons learned from additional areas of best practice (e.g., measurement, risk management, and supplier management)
- Implement more robust high-maturity practices
- Address additional organizational functions critical to their products and services
- More fully comply with relevant ISO standards

Embracing a process view

- Improvement in meeting resiliency goals is dependent on the active management and measurement of the process
- Process maturity increases capability for meeting goals and sustaining the process
- *"Are we resilient?"* or *"Are we secure?"* is answered in the context of goal achievement rather than **what hasn't happened**
- Facilitates meaningful, purposeful selection and implementation of practices

Process Areas

22 in CMMI 1.2

- Grouped into four sets:
  - Process Management
  - Project Management
  - Engineering
  - Support
- Measurement and Analysis are one Process Area

Processes Areas, Goals, and Practices

CMMI Measurement and Analysis Process Area

Measurement and Analysis Process Area

Purpose -develop and sustain a measurement capability that is used to support management information needs.

The measurement and analysis process area involves:

- Specifying the objectives of measurement and analysis such that they are aligned with identified information needs and objectives
- Specifying the measures, analysis techniques, and mechanisms for data collection, data storage, reporting, and feedback.
- Implementing the collection, storage, analysis, and reporting of the data
- Providing objective results that can be used in making Informed decisions, and taking appropriate corrective actions

Measurement and Analysis Process Area$_2$

When Measurement and Analysis is not done well …

Measurements are used inappropriately

Inappropriate measures can cause unintended behavior

Management is based on perception, rather than fact.

Measurement presentations may confuse rather than enlighten

Useless measures are collected

Measurement and Analysis Process Area$_3$

SG1 Align Measurement and Analysis Activities

- SP1.1 Establish measurement objectives
- SP 1.2 Specify measures
- SP 1.3 Specify data collection and storage procedures
- SP 1.4 Specify analysis procedures

SG 2 Provide measurement results

- SP2.1 Collect measurement data
- SP 2.2 Analyze measurement data
- SP 2.3 Store data and results
- SP2.4 Communicate results

Measurement and Analysis Process Area
Specific Goal 1: Align Measurement and Analysis Activities

The Specific Practices listed under Specific Goal 1 may be addressed concurrently or in any order.

Measurement objectives and activities are aligned with identified information needs and objectives.

SP 1.1 Establish measurement objectives

SP 1.2: Specify measures

SP 1.3: Specify data collection and storage procedures

SP 1.4: Specify analysis Procedures

Measurement and Analysis Process Area
Specific Practice 1.1 Establish Measurement Objectives

Establish and Maintain measurement objectives that are derived from identified information needs and objectives

Ask yourself what question you are answering with the data, why you are measuring something, and how these measurements will affect behavior.

Activities:

- Document information needs and objectives
- Prioritize information needs and objectives
- Document, review, and update measurement objectives
- Provide feedback for refining and clarifying information needs and objectives as necessary
- Maintain traceability of measurement objectives to the identified information needs and objectives

Measurement and Analysis Process Area
Specific Practice 1.2: Specify Measures

Specify measures to address the measurement objectives

Base measure - obtained by direct measurement

- Ex: estimates and actual measures of effort and cost (number of person-hours)

Derived Measures- combine two or more base measures

- Usually expressed as ratios or other aggregate measures.

Activities include:

- Identify candidate measures based on documented measurement objectives
- Identify existing measures that already address the measurement objectives
- Specify operational definitions for the measures
- Prioritize, review, and update measures

Measurement and Analysis Process Area
Specific Practice 1.3: Data Collection and Storage Procedures

Specify how measurement data will be obtained and stored

Ensuring appropriate accessibility and maintenance of data integrity are two key concerns related to storage and retrieval

Activities:

- Identify existing sources of data that are generated from current work products
- Identify measures for which data are needed, but are not currently available
- Specify how to collect and store the data for each required measure
- Create data collection mechanisms and process guidance
- Support automatic collection of data where appropriate and feasible
- Prioritize, review, and update data collection and storage procedures
- Update measures and measurement as necessary

Measurement and Analysis Process Area
Specific Practice 1.4: Specify Analysis Procedures

Specify how measurement data will be analyzed and reported

Activities:

- Specify and prioritize the analysis that will be conducted and the reports that will be prepared
- Select appropriate data analysis methods and tools
- Specify administrative procedures for analyzing the data and communicating the results
- Review and update the proposed content and format of the specified analyses and reports
- Update measures and measurement objectives as necessary
- Specify criteria for evaluating the utility of the analysis results and for evaluating the conduct of measurement and analysis activities

Measurement and Analysis Process Area
Specific Goal 2: Provide Measurement Results

SG 2 Provide Measurement Results

- SP2.1 Collect measurement data
- SP 2.2 Analyze measurement data
- SP 2.3 Store data and results
- SP2.4 Communicate results

Measurement and Analysis Process Area
Specific Goal 2: Provide Measurement Results$_2$

Measurement results, which address identified information needs and objectives, are provided.

Measurement results can:

- Monitor performance
- Fulfill contractual obligations
- Fulfill regulatory requirements
- Help make informed management and technical decisions
- Enable corrective actions to be taken

Measurement and Analysis Process Area
Specific Practice 2.1 Collect Measurement Data

Obtain specified measurement data

Activities:

- Obtain the data for base measures
- Generate the data for the derived measures
- Perform data integrity checks as close to the source of the data as possible

Measurement and Analysis Process Area
Specific Practice 2.2 Analyze Measurement Data

Analyze and interpret measurement data

Activities

- Conduct initial analyses, interpret results, and draw preliminary conclusions
- Conduct additional measurement and analyses as necessary, and present results
- Review the initial results with relevant stakeholders
- Refine criteria for future analyses

Measurement and Analysis Process Area
Specific Practice 2.3: Store Data and Results

Manage and store measurement data, specifications, and analysis results

- Information stored typically includes:
  - Measurement Plans
  - Specifications of measures
  - Sets of data that have been collected
  - Analysis reports and presentations

Activities:

- Review the data to ensure their completeness, integrity, accuracy, and currency
- Store the data according to the data storage procedures
- Make the stored contents available for use only by appropriate groups and personnel
- Prevent the stored information from being used inappropriately

Measurement and Analysis Process Area
Specific Practice 2.4 Communicate Results

Report results of measurement and analysis activities to all relevant stakeholders.

Activities:

- Keep relevant stakeholders apprised of measurement results on a timely basis
- Assist relevant stakeholders in understanding the results

Generic Goals

Perform the Specific Practices

Institutionalize the Managed Process

- Establish an organizational policy
- Plan the process
- Provide resources
- Assign responsibilities
- Train people
- Manage configurations
- identify and Involve relevant stakeholders
- Monitor and control the process

Generic Goals$_2$

- Objectively evaluate adherence
- Review status with high level management

Institutionalize a defined process

- Establish a defined process
- Collect improvement information

Institutionalize a quantitatively managed process

- Establish quantitative objectives for the process
- Stabilize subprocess performance

Institutionalize an optimizing process

- Ensure continuous process improvement
- Correct root causes of problems

Summary and Conclusion

“Lessons Learned” in measurement and metrics

- “Measurement is a consistent but flexible process that must be tailored to the unique information needs and characteristics of a particular organization.
- Decision makers must understand what is being measured.
- Measurements must be used to be effective.

A large number of measurement programs fail early in their inception, usually because they do not provide relevant information to user needs.*”

* “Making Measurement Work” Cheryl Jones, STSC Crosstalk

“Lessons Learned” in measurement and metrics$_2$

- “Recognize that implementation of a measurement program may take a long time and that management can have a short-term window. Therefore, plan to show some short-term successes before management change. Start small and build upon success.
- Pay close attention to privacy issues pertaining to who can see what portion of the data.

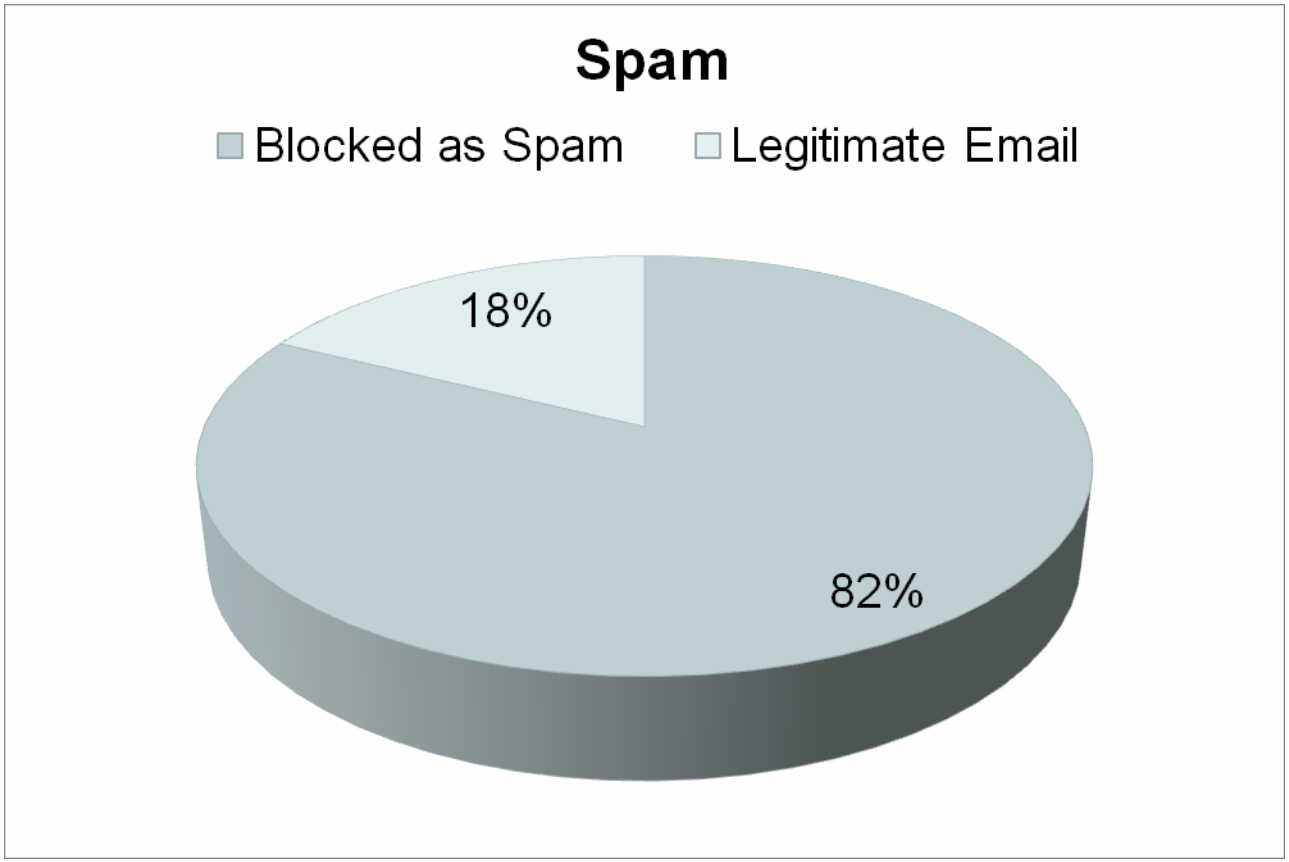
* “Experiences in Implementing Measurement Programs” W. Goethert, W. Hayes, Software Engineering Institute, 2001 http://www.sei.cmu.edu/publications/documents/01.reports/01tn026.html

"Lessons Learned" in measurement and metrics$_3$

- "A good metric is based upon F.A.C.T. –
  - Flexible
  - Accurate
  - Context-sensitive
  - Transparent*
- Major obstacles that appear when implementing a program are a result of an unreliable process for defining what needs to be measured, when it needs to be measured, and how the results can be derived, communicated, and interpreted.*"

- ""Why are Security Metrics a Necessity for Organizations" E. Nichols, ClearPoint Metrics, March, 2006 http://www.clearpointmetrics.com/newsite/Generic/default.aspx?ID=112

Applying the Lessons



Applying the Lessons$_2$

Our strategic Goal is "*To improve electronic communications between employees and customers.*" we achieve this through:

1. Ensuring the availability of our email infrastructure (uptime)
2. Providing protection against unwanted communications (viruses, spam, phishing)
3. Promoting responsible email communications (compliance, education)

Measures of Success:

- **Systems availability**
  - in 1st quarter, email infrastructure uptime = 89.5 days out of 90 days (99.4%)
- **Unwanted messages**
  - Total mail in 1st quarter = 15,690
  - Total messages blocked as "unwanted" = 12,915 (82%)
- **Promoting responsible communication:**
  - 100% outgoing messages have disclaimers
  - Web page tutorial "safe email communications" completed (100% implemented)

Summary and Conclusion

Information security measurement program needs:

- Strong management support
- Practical policies and procedures
- Quantifiable performance measures
- Results-oriented measure analysis

There are three types of information security metrics:

- Implementation
- Effectiveness/efficiency
- Impact

Summary and Conclusion$_2$

The maturity of an agency's program will determine what type of metric it will find to be the most useful

The metrics development process has seven phases:

- Identification of stakeholders
- Identification of goals and objectives
- Security policy and procedure review
- System security plan Implementation review
- Metrics development and selection
- Establishing performance targets
- Feedback and refinement

Summary and Conclusion$_3$

NIST SP 800-55 is the only issued guidance, and that focuses primarily on individual systems. SP800-80 was released as a draft, and will not be issued as a final publication.

SP 800-55 R1 integrates 800-55 and 800-80, focusing not only on individual systems, but on enterprise information security management programs.

Due to the unique nature of metrics to their organization, there is no "one size fits all" solution, although the NIST documents have some suggestions to get programs started.

If the NIST approach is not the right one for your organization, there are other approaches, such as the CMMI.

Bibliography

- "**Metrics 101**" presentation by Elizabeth A. Nichols, CTO ClearPoint metrics, May 2006
- "**Security Metrics: Replacing Fear, Uncertainty, and Doubt**" Andrew Jaquith © 2007 Pearson Education, inc.
- "**Making Measurement Work**" Cheryl Jones, STSC Crosstalk http://www.stsc.hill.af.mil/Crosstalk/2003/01/jones.html
- "**Experiences in Implementing Measurement Programs"** W. Goethert, W. Hayes, Software Engineering Institute, 2001 http://www.sei.cmu.edu/publications/documents/01.reports/01tn026.html
- "**Why are Security Metrics a Necessity for Organizations**" E. Nichols, ClearPoint Metrics, March, 2006 http://www.clearpointmetrics.com/newsite/Generic/default.aspx?ID=112
- **CMMI® Second Edition: Guidelines for Process Integration and Product Improvement**" Mary Beth Chrissis, Mike Konrad, Sandy Shrum, © 2007 Pearson Education, Inc

CMMI ® Registration Notice

CMM, CCMI, Capability maturity Model, Capability Maturity Modeling, Carnegie Mellon, CERT, and CERT Coordination Center are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University

CMMI® material used in this presentation has been taken from:

"**CMMI® Second Edition: Guidelines for Process Integration and Product Improvement**" Mary Beth Chrissis, Mike Konrad, Sandy Shrum, © 2007 Pearson Education, Inc

Some CMMI – slides taken from the SEI "Introduction to CMMI v1.2 – 070207" presentation, copyright 2007, Carnegie Mellon University

For more information

Samuel A. Merrell, CISSP, GSEC, GGSC

Software Engineering Institute
Carnegie Mellon University

www.sei.cmu.edu

www.cert.org

smerrell@cert.org